Cryptography and Network Security

Introduction to Advanced Encryption Standard (AES)

Outcomes

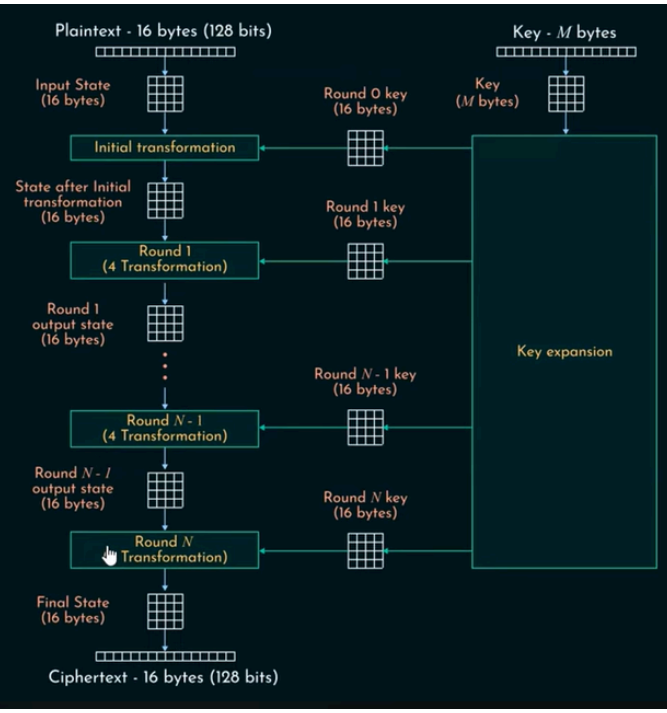
Upon the completion of this session, the learner will be able to

- ★ Understand the basics of AES.
- ★ Know the basic differences between DES and AES.
- ★ Know the AES structure.
- ★ Know the AES parameters.

AES

- Advanced Encryption Standard.
- NIST in 2001.
- Symmetric block cipher.
- Widely used.

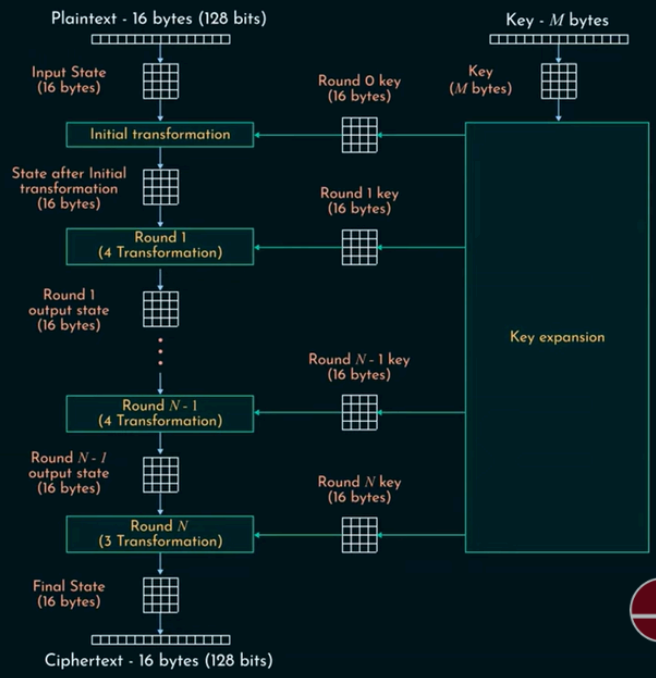
AES Structure



nesoacademy.org

AES Structure

No. of rounds	Key size (in bits)
10	128
12	192
14	256



nesoacademy.org

AES Parameters

	AES-128	AES-192	AES-256
Key Size	128	192	256
Plaintext Size	128	128	128
Number of rounds	10	12	14
Round Key Size	128	128	128

Cryptography and Network Security

AES Encryption and Decryption

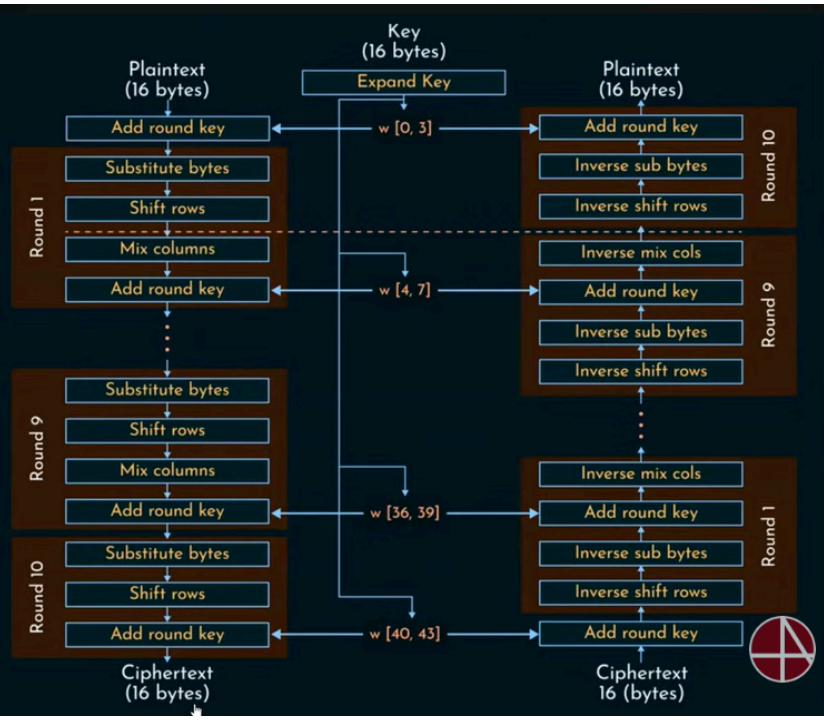
nesoacademy.org

Outcomes

Upon the completion of this session, the learner will be able to

- ★ Recall the AES structure and the relationship between the key size and number of rounds.
- ★ Understand the AES encryption and decryption.
- ★ Know the various transformations in AES encryption and decryption process.

AES Encryption and Decryption



nesoacademy.org

Cryptography and Network Security

AES Round Transformation

nesoacademy.org

Outcomes

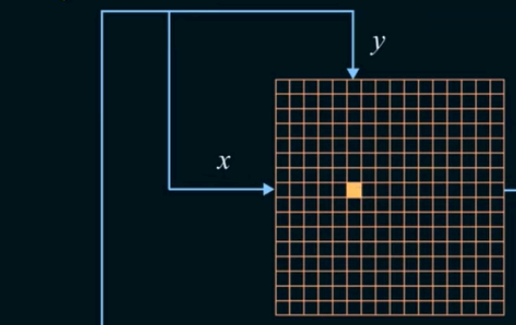
Upon the completion of this session, the learner will be able to

- ★ Understand the four transformations in AES encryption and decryption process.

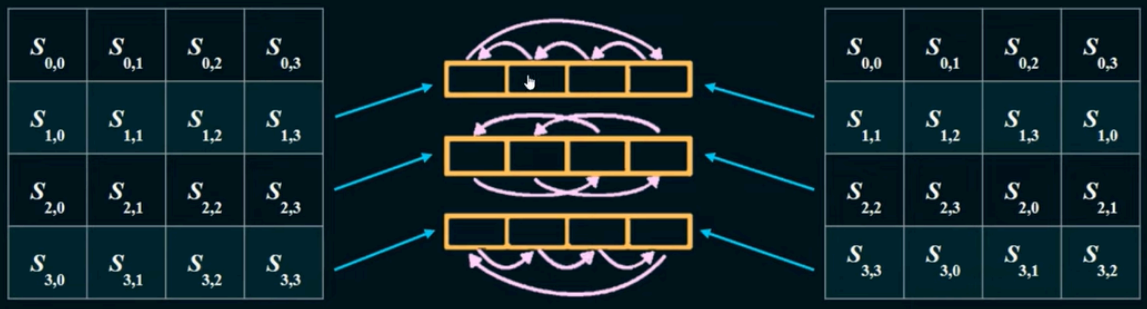
AES Transformation Functions

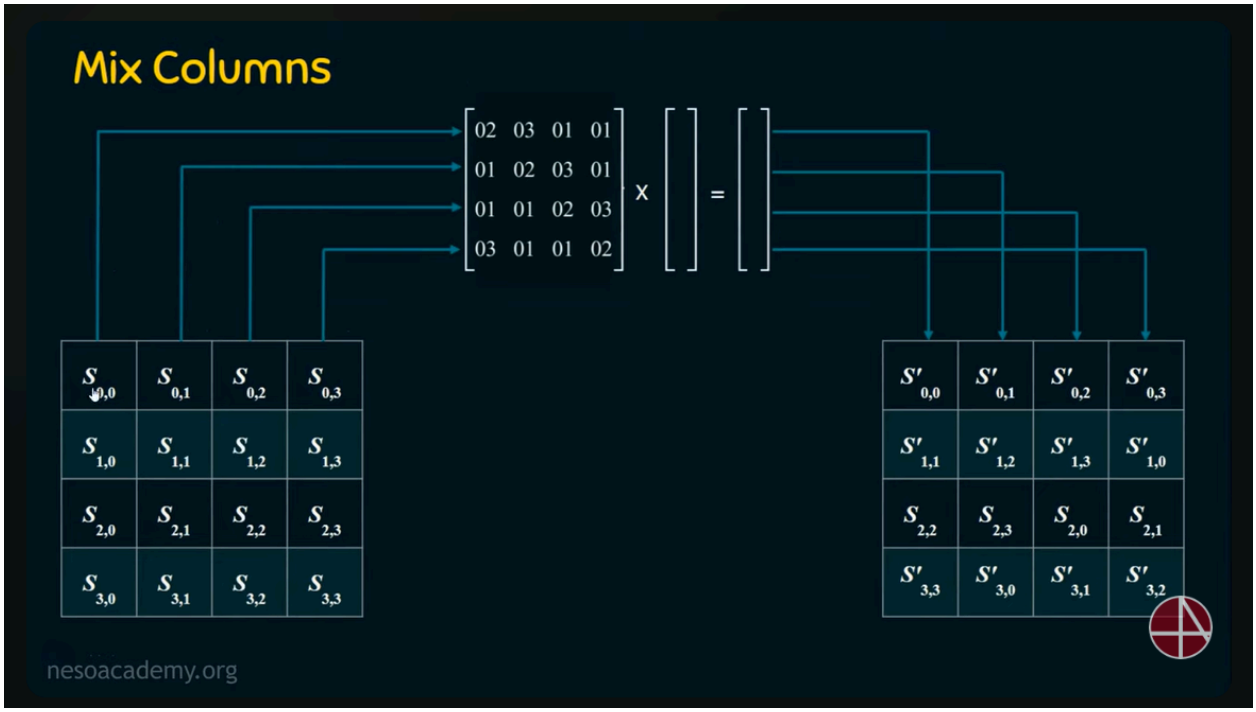
- ★ Substitute Bytes
- ★ Shift Rows
- ★ Mix Columns
- ★ Add Round Key

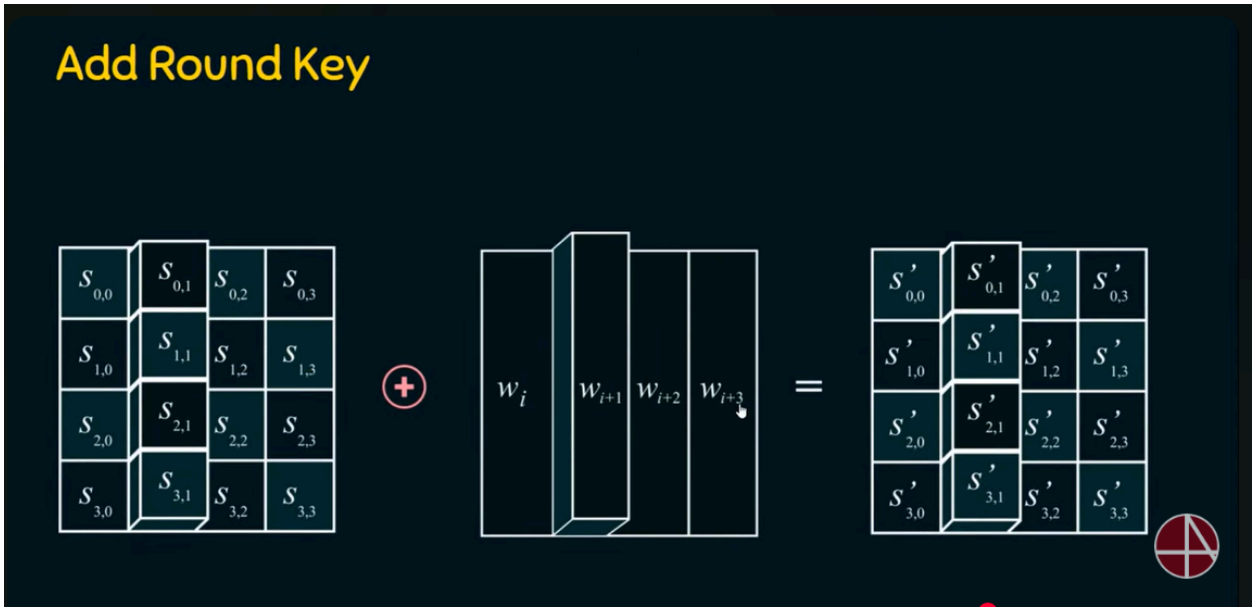
Substitute Bytes



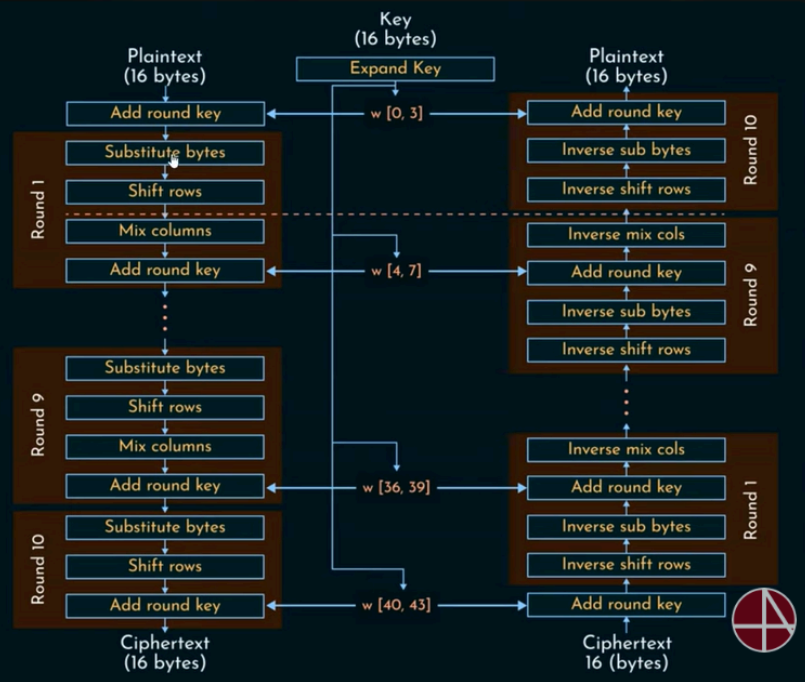
Shift Rows




Mix Columns
02 03 01 01
01 02 03 01
01 01 02 03
03 01 01 02
x
=
nesoacademy.org


Add Round Key
w_i
w_{i+1}
w_{i+2}
w_{i+3}
=

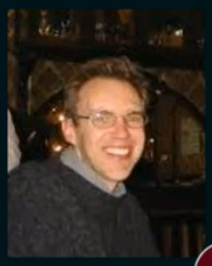
AES Encryption and Decryption



AES

- Rijndael cipher.
- Rijndael was selected as the AES in Oct-2000.
- Designed by Vincent Rijmen and Joan Daemen in Belgium.
- Simplicity.
- 128/192/256 bit keys, 128 bits data.

V. Rijmen



J. Daemen

AES Security

- AES was designed after DES.
- Most of the known attacks on DES were already tested on AES.
- Brute-Force Attack.
- Statistical Attacks.
- Differential and Linear Attacks.

AES Implementation Aspects

- Simple Algorithms.
- Resistant against known attacks.
- Code compactness on many CPUs.
- Cheap processors and minimum amount of memory.
- Very efficient.
- Implementation of AES.

AES Example

https://www.cryptool.org/en/cto/aes-step-by-step